REMARKS

The foregoing amendments and the following remarks are responsive to the Office Action mailed July 28, 2005. In the Office Action, claims 1-26 were pending and claim 1-26 were rejected. In this response, claims 1-3, 7, 8, 10, 17, 20-22, and 25 have been amended. No new matter has been added by these amendments. Applicants respectfully request reconsideration of the present application.

The Examiner rejected claims 2, 7-9 and 17-24 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Applicants respectfully submit that claim 2, 7-9, and 17-24, as amended, satisfy the requirements of 35 U.S.C. § 112, second paragraph, and respectfully request the withdrawal of the rejection of claim under § 112. The Applicants, however, did not amend the claims in response to rejections 'b' and 'q' for the following reasons. With respect to rejection 'b', claim 3 depends on claim 2 which recites "an application." With respect to rejection 'q', claim 25 recites the abbreviation "disk ID" on line 4 of the claim to which "the disk ID" refers. As such, the Applicants submit there was no need to amend claim 3 and 25 to overcome the rejections under §112.

Examiner rejected claim 1-6 and 10-16 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,499,106 to Yaegashi et al. (hereinafter "Yaegashi") in view of Handbook of Applied Cryptography by Menezes et al. (hereinafter "Menezes").

With respect to amended claim 1, the Applicants claim:

> determining a secure medium identification (disk ID) from a secure medium including content;
> sending a encrypted one-time session key and the disk ID to a server;
> requesting user authentication; and
> if the user is successfully authenticated, receiving a decrypted copy of the encrypted one-time session key from the server to enable reading of the content on the secure medium.

if the user is successfully authenticated, receiving a decrypted copy of the encrypted one-time session key from the server to enable reading of the content on the secure medium.

Applicants respectfully disagree with the rejection because the references fail to teach or suggest, alone or in combination, that "if the user is successfully authenticated, receiving a decrypted copy of the encrypted one-time session key from the server to enable reading of the content on the secure medium."

Yaegashi describes delivering secured disks to a known location where each location is associated with a unique location ID number (Yaegashi, Column 9, lines 20-54). Then when a user desires to view content on the disk, the user transmits a disk ID number and the unique location ID to a central access control system (Yaegashi, column 9, lines 46-54). A user must provide both the disk ID and the location ID to obtain a decryption key for data on the disk (Yaegashi, column 12, lines 20-33). The decryption key is itself encrypted with the unique location ID and transmitted to the user. However, the key encrypted by the location ID allows the user to store the decryption key for all future uses of the disk without needing to reacquire the decryption key (Yaegashi, column 12, lines 51-61).

Menezes further describes a system for facilitating secure communications between two users through a management system (Menezes, page 533, section 13.3.2). The system can either be used to transfer messages or keys once a user has initially provided a key to the system (Menezes, page 553, section 13.3.2). However, a user can replay a message or decrypt a key previously received, because the protocols as described provide no entity authentication (Menezes, page 554, section 13.13).

The Applicants, however, describe that upon user authentication, a one-time session key is received by a user to allow decrypting of content using the one-time key. Because Yaegashi and Menezes provide a decryption key to a user, which allows the user to decrypt the content at any time in the future, neither Yaegashi nor Menezes, alone or in combination, teach or suggest all of the limitation claimed in amended claim 1. Furthermore, because claims 2-6 and 10-16 contain features that further limit independent claim 1, claims 2-6 and 10-16 are also not rendered obvious under 35 U.S.C. § 103(a) over Yaegashi in view of Menezes. Thus, the Applicants respectfully request withdrawal of the rejections.

The Examiner rejected claims 17 and 18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,636,966 to Lee et al. (hereinafter "Lee") in view of U.S. Patent No. 6,236,727 to Ciacelli et al. (hereinafter "Ciacelli") in further view of Applied Cryptography, Second Edition, by Schneier.

With respect to claim 17, the Applicants claim "a reader to read an identification (ID) and content from a secure medium; a session key generation logic to generate a one-time session key; [and] an encryption logic to send the ID and the session key encrypted to a server." Applicants respectfully disagree with the rejection because the references fail to teach or suggest, alone or in combination, that an apparatus for accessing secure content includes "a session key generation logic to generate a one-time session key; [and] an encryption logic to send the ID and the session key encrypted to a server" as claimed in claim 17.

Lee describes a system to enable a user to pay for all or part of the content available on an encrypted medium (Column 5, lines 4-23). To access the encrypted information

selected by the user, the user establishes a session ID with a server, which is merely an ID to track the user's activity during the present financial transaction (Column 8, lines 56-60). Lee further describes that a user can enter information, such as a credit card number or demographic information, in order to send it to a content key server (Column 5, line 55 to Column 6, line 3). If the user information is accepted by the content key server, the user receives a decryption key that is permanently stored to access information that the user purchased (Column 5, lines 45-53).

Ciacelli, on the other hand, describes processing an encrypted data stream to protect copyrighted material during electronic transmission of that data (Abstract and Column 3, lines 44-54). If it is determined that content must be encrypted to protect an existing copyright, software scrambles/encrypts the content before sending it (Column 4, lines 32-53). As such, Ciacelli merely describes encrypting content before transmitting it. As noted in Ciacelli, the content can be encrypted according to methods described in Schneier. Schneier describes the use of a session key algorithm to allow encryption for one communication session (Page 180). As such, content can be encrypted with a session key before it is transmitted.

However, neither Lee, Ciacelli, nor Schneier, alone or in combination describe an apparatus which includes both a session key generation logic to generate a one-time session key and an encryption logic to send the ID and the session key encrypted to a server. Whereas Lee merely describes allowing a user to obtain a decryption key by sending user information to a server, Ciacelli and Lee only describe encrypting a content data stream with a session key. Thus, the references, alone or in combination, fail to teach or suggest sending an encrypted ID and session key to a server, as claimed in Claim 17. Thus, claim 17 is not rendered obvious under 35 U.S.C. § 103(a) for at least the reasons discussed above. Furthermore, since claim 18 contains features that further limit claim 17, claim 18 is also not

rendered obvious under § 103(a), for at least the same reasons. The Applicants respectfully request withdrawal of the rejections.

The Examiner rejected claims 20 and 21 under 35 U.S.C. § 103(a) as being unpatentable over Lee, Ciacelli, and Schneier, as applied to claim 17, and further in view of Yaegashi. The Applicants respectfully disagree with the rejections. As discussed above, Lee, Ciacelli, and Schneier fail to teach or suggest each and every element as claimed in claim 17. Furthermore, Yaegashi fails to describe or suggest the use of a session key, as discussed above with respect to claim 1. Thus for similar reasons, Yaegashi also fails to teach or suggest the use of a session key as claimed in claim 17. Therefore, Lee, Ciacelli, Schneier, and Yaegashi, alone or in combination fail to describe or suggest each and every element as claimed by the applicants in claims 20 and 21. The Applicants respectfully request withdrawal of the rejections.

The Examiner rejected claim 25 under 35 U.S.C. § 103(a) as being unpatentable over Yaegashi in view of Ciacelli. The Applicants respectfully disagree as the references, alone or in combination, fail to teach or suggest each and every element as claimed in claim 25.

With respect to amended claim 25, the Applicants claim:

> an association logic to determine if the disk ID is associated with the user, and;
> if the disk ID is not yet associated with the user, to associate the user authentication data with the disk ID; and
> if the disk ID is associated with the user, determining that the current user authentication matches the user associated with the disk ID, to authenticate the user;

The Applicants respectfully disagree with the rejection because neither Yaegashi, nor Ciacelli, alone or in combination teach or suggest an association logic that associates a disk ID with a user.

Yeagashi, similar to the description above, describes a system where

disks are distributed with disk IDs and unique location identification numbers. Although a user must log into an access system to view a disk, the system merely determines whether the decryption key associated with the unique location code has already been obtained (Yaegashi, Column 12, lines 4-17). Thus, each disk ID is only associated with its corresponding unique location identification number (Yaegashi, Column 10, lines 40-65). Ciacelli, on the other hand, associates content with the need to protect content, i.e. as required by copyright (Ciacelli, Column 5, line 65 to column 6, line 11). Therefore, neither Yaegashi nor Ciacelli, alone or in combination teach or suggest an association logic to associate a disk ID with a user, as claimed in claim 25. The Applicants respectfully request withdrawal of the rejection.

The Examiner further rejected claim 26 under 35 U.S.C. § 103(a) as being unpatentable over Yaegashi and Ciacelli, as applied to claim 25 above, and further in view of Schneier. As discussed above, neither Yaegashi nor Ciacelli teach or suggest the association unit as claimed in claim 25. Furthermore, Schneier merely describes encryption methods and various encryption keys. As such, Scheier also fails to teach or suggest an association logic that associates a disk ID with a user, as claimed by the Applicants in claim 25. Thus, since claim 26 depends from and contains features that further limit claim 25, and none of the references, alone or in combination teach or suggest the limitations as claimed in claim 25, claim 26 is also not rendered obvious by the references for at least the reasons discussed above with respect to claim 25. The Applicants respectfully request withdrawal of the rejection.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that all pending claims are in condition for allowance. Such allowance is respectfully requested.

If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Judith A. Szepesi at (408) 720-8300.

If there are any additional charges, please charge Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR ZAFMAN LLP

Date: 10/26/05

Judith A. Szepesi
Reg. No, 39,393

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300